

Bounds for Signature Codes

Arkadii D'yachkov*, Nikita Polyanskii[†], Vladislav Shchukin*, and Ilya Vorobyev*

*Lomonosov Moscow State University, Moscow, Russia

[†]Institute for Information Transmission Problems, Moscow, Russia

agd-msu@yandex.ru, nikitapolyansky@gmail.com, vpike@mail.ru, vorobyev.i.v@yandex.ru

Abstract—We discuss upper and lower bounds of the zero error capacity for signature codes based on the symmetric noiseless multiple access channel.

Keywords: Multiple access channel (MAC), signature code, symmetric MAC, compositional MAC, joinable MAC, disjunctive MAC, information-theoretic bounds, random coding bounds.

I. STATEMENT OF PROBLEM

A. Notations

Let q, N, t, s and L be integers, $q \geq 2, N \geq 2, 2 \leq s < t, 1 \leq L \leq t - s$, the symbol \triangleq denotes the equality by definition, $\mathcal{A}_q \triangleq \{0, 1, \dots, q-1\}$ – the standard q -nary alphabet, $[N] \triangleq \{1, 2, \dots, N\}$ – the set of integers from 1 to N and $|A|$ – the size of the set A . A q -nary $(N \times t)$ -matrix

$$\begin{aligned} X_q &= \|x_i(j)\|, \quad x_i(j) \in \mathcal{A}_q, \quad i \in [N], j \in [t], \\ \mathbf{x}(j) &\triangleq (x_1(j), \dots, x_N(j)) \in \mathcal{A}_q^N, \\ \mathbf{x}_i &\triangleq (x_i(1), \dots, x_i(t)) \in \mathcal{A}_q^t \end{aligned} \quad (1)$$

with t columns (codewords) $\mathbf{x}(j), j \in [t]$, and N rows $\mathbf{x}_i, i \in [N]$, is called a q -nary code of length N and size $t = \lfloor q^{RN} \rfloor$, where a fixed parameter $R > 0$ is called a rate of the code X_q .

For a q -nary column $\mathbf{x} = (x_1, \dots, x_N) \triangleq \mathbf{x}_1^N \in \mathcal{A}_q^N$, define the vector of integers $[N_0, \dots, N_{q-1}]$, where $N_a = N_a(\mathbf{x})$, $0 \leq N_a \leq N$, $a \in \mathcal{A}_q$, is the number of positions $i, i \in [N]$, in which $x_i = a$. Obviously, $\sum_{a=0}^{q-1} N_a = N$. The vector $[N_0, \dots, N_{q-1}]$, is said to be a composition¹ of the q -nary vector $\mathbf{x}_1^N = (x_1, \dots, x_N) \in \mathcal{A}_q^N$ or, briefly,

$$\text{comp}(\mathbf{x}_1^N) \triangleq [N_0, \dots, N_{q-1}]. \quad (2)$$

Note that the number of all compositions is equal to $\binom{N+q-1}{q-1}$ and the number of all distinct q -nary columns $\mathbf{x} = (x_1, \dots, x_N) \in \mathcal{A}_q^N$ having the same composition (2) is equal to $N!/N_0! \dots N_{q-1}!$. Code X_q is said to be a fixed-composition code if all codewords $\mathbf{x}(j), j \in [t]$, have the same composition $[N_0, \dots, N_{q-1}]$.

Let $\mathbf{e} \triangleq \{e_1, \dots, e_s\}, 1 \leq e_1 < \dots < e_s \leq t$, be an arbitrary s -subset of $[t]$. Introduce $\mathcal{E}(s, t)$ as the set of all such subsets. Note that the cardinality $|\mathcal{E}(s, t)| = \binom{t}{s}$. For the given s -subset $\mathbf{e} = \{e_1, \dots, e_s\}$ called a message, consider a non-ordered s -collection of codewords (subcode)

$$\mathbf{x}(\mathbf{e}) \triangleq \{\mathbf{x}(e_1), \dots, \mathbf{x}(e_s)\}. \quad (3)$$

¹In the well-known book [1], the authors use the term *type*.

We say that $\mathbf{x}(\mathbf{e})$ encodes the message \mathbf{e} . If

$$\mathbf{x}_i(\mathbf{e}) \triangleq (x_i(e_1), \dots, x_i(e_s)) \in \mathcal{A}_q^s, \quad i \in [N], \quad (4)$$

is the i -th row of s -collection $\mathbf{x}(\mathbf{e})$, then the subcode (3) can be written as the N -collection of rows (4), i.e., $\mathbf{x}(\mathbf{e}) = \{\mathbf{x}_1(\mathbf{e}), \dots, \mathbf{x}_N(\mathbf{e})\}$.

B. Multiple Access Channel and Signature Codes

We will use the terminology of a noiseless (deterministic) multiple-access channel (MAC), which has s inputs and one output [1]. Let all s input alphabets of MAC be the same and coincide with the alphabet $\mathcal{A}_q \triangleq \{0, 1, \dots, q-1\}$. Denote by Z the finite output alphabet of size $|Z|$. The noiseless MAC is prescribed by the function

$$z = f(x_1, \dots, x_s) \triangleq f(\mathbf{x}_1^s), \quad z \in Z, \quad \mathbf{x}_1^s \in \mathcal{A}_q^s. \quad (5)$$

or by the following conditional probability

$$\tau^{(f)}(z|\mathbf{x}_1^s) \triangleq \begin{cases} 1 & \text{if } z = f(x_1, \dots, x_s) \\ 0 & \text{if } z \neq f(x_1, \dots, x_s) \end{cases} \quad (6)$$

on the Cartesian product $\mathcal{A}_q^s \times Z$.

Let the row $\mathbf{x}_i(\mathbf{e}), i \in [N]$, defined by (4), be the s -collection of signals at s MAC inputs at the i -th time unit. Then the signal $z_i, z_i \in Z, i \in [N]$, at the output of MAC at the i -th time unit is

$$z_i = z_i^{(f)}(\mathbf{e}, X_q) \triangleq f(x_i(e_1), \dots, x_i(e_s)) \in Z. \quad (7)$$

The deterministic model of MAC is called an f -MAC.

On the base of the code X_q (1) and N signals

$$\mathbf{z}^{(f)}(\mathbf{e}, X_q) \triangleq (z_1^{(f)}(\mathbf{e}, X_q), \dots, z_N^{(f)}(\mathbf{e}, X_q)) \in Z^N,$$

which are known at the output of MAC, an observer makes the brute force decision about the unknown message \mathbf{e} . To identify \mathbf{e} , a code X_q (1) is assigned

Definition 1. [2], [3]. A q -nary code X_q is said to be a signature (s, q) -code, of size t and length N for the f -MAC if all $\mathbf{z}^{(f)}(\mathbf{e}, X_q), \mathbf{e} \in \mathcal{E}(s, t)$ are distinct.

The signature code allows to solve an identification problem of active users, arising in some communication nets. For instance, more detailed descriptions of the problem can be found in [3], [4].

Let $t^{(f)}(s, q, N)$ be the maximal size of signature (s, q) -codes of length N for the f -MAC. For fixed $s \geq 2$ and $q \geq 2$, define the number

$$R^{(f)}(s, q) \triangleq \overline{\lim}_{N \rightarrow \infty} \frac{\log_q t^{(f)}(s, q, N)}{N}, \quad (8)$$

called a *rate* of signature (s, q) -codes for the f -MAC. Using the terminology of the Shannon coding theory, the number $R^{(f)}(s, q)$ can be called a *zero error capacity* of signature codes for the f -MAC.

Definition 2. [2], [5], [6]. An f -MAC given by (5) is said to be the *symmetric* f -MAC if any of $s!$ permutations $\pi = \pi(k)$, $k \in [s]$, on the set $[s]$, satisfies the equality

$$f(x_1, \dots, x_s) = f(x_{\pi(1)}, \dots, x_{\pi(s)}), \\ \pi(k) \in [s], k \in [s], \quad \pi(k) \neq \pi(k'), k \neq k'. \quad (9)$$

In other words, the equality (9) means that the f -MAC is the symmetric f -MAC if the function $z = f(x_1^s)$ does not depend on the order of arguments (x_1, \dots, x_s) .

In Sect. I-C-I-F, we introduce four models of the symmetric f -MAC which, by our opinion, can be considered as the most important for applications.

C. Compositional MAC

The symmetric f -MAC is said to be the *compositional* MAC (briefly, *comp*-MAC) if

$$z = f(x_1^s) \triangleq \text{comp}(x_1^s). \quad (10)$$

where the compositional function $\text{comp}(x_1^s)$ is defined by (2). One can easily see that the size of output alphabet for the *comp*-MAC is $|Z| = \binom{q+s-1}{s}$. Using the permutation symbol $\pi = \pi(k)$ (9) the necessary and sufficient condition for the coincidence of signals $\text{comp}(x_1^s)$ and $\text{comp}(y_1^s)$ at the output of the *comp*-MAC can be written in the form:

$$\text{comp}(x_1^s) = \text{comp}(y_1^s) \iff \\ \iff \bigcup_{\pi} \left[\bigcap_{k=1}^s (x_k = y_{\pi(k)}) \right] \neq \emptyset, \quad (11)$$

where the right-hand side of (11) says that for a vector x_1^s , $x_1^s \in \mathcal{A}_q^s$, there exists a permutation $\pi = \pi(k)$, $k \in [s]$, remaining the $\text{comp}(x_1^s)$.

D. Joinable MAC

The given symmetric f -MAC (briefly, *join*-MAC) is described by the function

$$z = f(x_1, \dots, x_s) \triangleq \bigcup_{i=1}^s x_i \subseteq \mathcal{A}_q.$$

We would like to note the paper [7], where the significant applications of the *comp*-MAC, called the *B*-channel, and the *join*-MAC, called the *A*-channel, were firstly developed. We also refer to [8]-[11], where the maximal output entropy [1], [7] of the *A*-channel and the *B*-channel was investigated in different asymptotic and non-asymptotic cases.

E. Erasure MAC

The q -nary, $q \geq 2$, symmetric f -MAC is said to be the *erasure* MAC (briefly, *eras*-MAC) if it has the $(q+1)$ -nary output alphabet $Z \triangleq \{0, 1, \dots, q-1, *\}$ and the output function $z = f(x_1^s)$ (5) has the form:

$$z = f(x_1, \dots, x_s) \triangleq \begin{cases} a & \text{if } x_1 = \dots = x_s = a, a \in \mathcal{A}_q, \\ * & \text{otherwise.} \end{cases}$$

The *eras*-MAC model can be considered as an adequate description for the transmission of q -nary symbols based on the *frequency modulation* method.

F. Disjunctive MAC

Such symmetric f -MAC (briefly, *disj*-MAC) has the binary ($q = 2$) input and output alphabets $Z \triangleq \mathcal{A}_2 = \{0, 1\}$ and

$$f(x_1, \dots, x_s) \triangleq \begin{cases} 1 & \text{if } \sum_{i=1}^s x_i > 0, \\ 0 & \text{if } \sum_{i=1}^s x_i = 0. \end{cases}$$

The *disj*-MAC model is interpreted as the transmission of binary symbols based on the *impulse modulation* method. In addition, the binary signature $(s, 2)$ -codes for the *disj*-MAC are closely connected with the *combinatorial search theory* [12] and the information-theoretic model called the *design of screening experiments* [6].

The outline of our paper is as follows. Sect. II reminds in the form of Propositions 1-3 the principally known information-theoretic results relative to upper and lower bounds on the rate $R^{(f)}(s, q)$ of signature (s, q) -codes for the general case of the symmetric f -MAC.

In Sect. III-A and III-B, we remind the best known [6], [13], [14] bounds on the rate $R^{(disj)}(s, 2)$ of signature $(s, 2)$ -codes for the disjunctive MAC and bounds on the rate $R^{(eras)}(s, q)$ of signature (s, q) -codes for the erasure MAC.

Theorem 1 proved in Sect. III-C gives a new combinatorial upper bound on the rate $R^{(f)}(s, q)$ of signature (s, q) -codes for any symmetric f -MAC.

In Sect. III-D, we study the asymptotic bounds on the rate $R^{(comp)}(s, q)$ of signature (s, q) -codes for the *comp*-MAC with large values of the parameters s and q and prove that the bound of Theorem 1 is approximately twice better than the classical entropy bound (15) of Proposition 1. Up to now, the possibility to improve the entropy bound (15) for the *comp*-MAC was established for the case $s = q = 2$ only (see, ref. in [6]). In addition, in Sect. III-D we prove Theorem 2 yielding a random coding lower bound on the rate $R^{(comp)}(s, q)$. If $s, q \rightarrow \infty$, then the comparison of upper and lower bounds of Theorems 1 and 2, leads to Corollary 1 which claims that $R^{(comp)}(s, q) \sim 1/2$.

The aim of Sect. IV is to discuss the concept of q -nary list-decoding signature codes for the joinable MAC. Such codes were introduced in the recent paper [15] as a further development of the concept of binary list-decoding disjunctive codes [13]. A combinatorial upper bound of Theorem 4 obtained in Sect. IV establishes the asymptotic ($q \rightarrow \infty$) precision of the random coding bound obtained in [15].

II. INFORMATION-THEORETIC BOUNDS

A. Entropy Upper Bound on $R^{(f)}(s, q)$

Let

$$\mathbf{p} \triangleq \left\{ p(a) : p(a) > 0, \sum_{a \in \mathcal{A}_q} p(a) = 1 \right\}, \quad (12)$$

be a fixed probability distribution at the alphabet \mathcal{A}_q and the vector $\xi_1^s \triangleq (\xi_1, \dots, \xi_s)$, $\xi_1^s \in \mathcal{A}_q^s$, is the s -collection of *independent* random variables having the same distribution (12), i.e., $\Pr\{\xi_k = a\} \triangleq p(a)$, $k \in [s]$, $a \in \mathcal{A}_q$. Introduce the corresponding Shannon entropy of the output of f -MAC, i.e.,

$$H_{\mathbf{p}}^{(f)}(s, q) \triangleq \sum_{z \in Z} \Pr\{f(\xi_1^s) = z\} \cdot \log_q \frac{1}{\Pr\{f(\xi_1^s) = z\}}. \quad (13)$$

Using the f -MAC definition (6), the probability in the right-hand side (13) can be written in the form

$$\Pr\{f(\xi_1^s) = z\} = \sum_{x_1^s} \tau^{(f)}(z|x_1^s) \cdot \prod_{k=1}^s p(x_k) \quad (14)$$

The following statement called the *entropy upper bound* on the rate $R^{(f)}(s, q)$ takes place.

Proposition 1. [2]. *The rate $R^{(f)}(s, q)$ of signature (s, q) -codes for the symmetric f -MAC satisfies the inequality*

$$R^{(f)}(s, q) \leq C^{(f)}(s, q) \triangleq \frac{\max_{\mathbf{p}} H_{\mathbf{p}}^{(f)}(s, q)}{s}. \quad (15)$$

B. Random Coding Error Exponent for the Symmetric f -MAC

Fix an arbitrary symmetric f -MAC. Given a code X_q , a message \mathbf{e} , $\mathbf{e} \in \mathcal{E}(s, t)$, is said to be *bad* for the code X_q , if there exists a message $\mathbf{e}' \neq \mathbf{e}$ such that $\mathbf{z}^{(f)}(\mathbf{e}', X_q) = \mathbf{z}^{(f)}(\mathbf{e}, X_q)$. If the unknown message \mathbf{e} is interpreted as the random vector taking equiprobable values in the set $\mathcal{E}(s, t)$, then the *relative number* of "bad" messages among all $\binom{t}{s} = |\mathcal{E}(s, t)|$ messages can be considered as the *error probability* of code X_q for the *brute force* decoding. Let the symbol $\mathcal{P}_N^{(f)}(s, t, [N_0, \dots, N_{q-1}])$ denote the *average error probability* over the *fixed composition ensemble* (briefly, *FC-ensemble*) of t independent q -nary codewords with the same composition $[N_0, \dots, N_{q-1}]$. By a similar symbol $\mathcal{P}_N^{(f)}(s, t, \mathbf{p})$ we will denote the *average error probability* over the *completely randomized ensemble* (briefly, *CR-ensemble*) of q -nary codes $X_q = \|x_i(j)\|$ (1) with independent components $x_i(j)$ having the same distribution \mathbf{p} (12), i.e., $\Pr\{x_i(j) = a\} \triangleq p(a)$, $i \in [N]$, $j \in [t]$, $a \in \mathcal{A}_q$.

Let a symmetric f -MAC is identified as the conditional probability $\tau^{(f)}(z|x_1^s)$ defined by (6). To present the results about the logarithmic asymptotic behavior of probabilities $\mathcal{P}_N^{(f)}(s, t, [N_0, \dots, N_{q-1}])$ and $\mathcal{P}_N^{(f)}(s, t, \mathbf{p})$, we need the following notations [6]. Let

$$\tau \triangleq \left\{ \tau(x_1^s, z) : \tau(x_1^s, z) \geq 0, \sum_{x_1^s, z} \tau(x_1^s, z) = 1 \right\} \quad (16)$$

be a probability distribution on the Cartesian product $\mathcal{A}_q^s \times Z$. Using the standard symbols for the conditional probabilities of the distribution τ (16), we denote by the symbol

$$\{\tau\}^{(f)} \triangleq \left\{ \tau : \tau^{(f)}(z|x_1^s) = 0 \Rightarrow \tau(z|x_1^s) = 0 \right\} - \quad (17)$$

the subset of probability distributions τ (16) such that the conditional probability $\tau(z|x_1^s) = 0$ if $\tau^{(f)}(z|x_1^s) = 0$.

Introduce the \cup -convex information-theoretic functions of the argument $\tau \in \{\tau\}^{(f)}$:

$$\begin{aligned} \mathcal{H}^{(f)}(\mathbf{p}, \tau) &\triangleq \sum_{x_1^s, z} \tau(x_1^s, z) \log_q \frac{\tau(x_1^s, z)}{\tau^{(f)}(z|x_1^s) \cdot \prod_{v=1}^s p(x_v)}, \\ I_k(\mathbf{p}, \tau) &\triangleq \sum_{x_1^s, z} \tau(x_1^s, z) \log_q \frac{\tau(x_1^k|x_{k+1}^s, z)}{\prod_{v=1}^k p(x_v)}, \quad k \in [s]. \end{aligned} \quad (18)$$

From (13) and (14), it follows that the distribution

$$\tau_{\mathbf{p}}^{(f)} \triangleq \left\{ \tau^{(f)}(z|x_1^s) \cdot \prod_{k=1}^s p(x_k), \quad x_1^s \in \mathcal{A}_q^s, \quad z \in Z \right\} \in \{\tau\}^{(f)}$$

and the functions (18) satisfy the equalities

$$\mathcal{H}^{(f)}(\mathbf{p}, \tau_{\mathbf{p}}^{(f)}) = 0, \quad I_s(\mathbf{p}, \tau_{\mathbf{p}}^{(f)}) = H_{\mathbf{p}}^{(f)}(s, q).$$

Put the symbol $[u]^+ \triangleq \max\{0; u\}$.

Proposition 2. [6]. *Let $s \geq 2$, $q \geq 2$, code rate $R > 0$ be fixed, and the entropy $H_{\mathbf{p}}^{(f)}(s, q)$ of a fixed distribution \mathbf{p} (12) is defined by (13). If code parameters N , $t \rightarrow \infty$ such that*

$$\frac{\log_q t}{N} \sim R, \quad \frac{N_a}{N} \sim p(a), \quad a \in \mathcal{A}_q, \quad s, q - \text{const},$$

then for the FC-ensemble there exists

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{-\log_q \mathcal{P}_N^{(f)}(s, t, [N_0, \dots, N_{q-1}])}{N} &\triangleq \\ &\triangleq E_{FC}^{(f)}(s, q, R, \mathbf{p}) > 0, \quad 0 < R < \frac{H_{\mathbf{p}}^{(f)}(s, q)}{s}, \end{aligned} \quad (19)$$

and for the CR-ensemble there exists

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{-\log_q \mathcal{P}_N^{(f)}(s, t, \mathbf{p})}{N} &\triangleq \\ &\triangleq E_{CR}^{(f)}(s, q, R, \mathbf{p}) > 0, \quad 0 < R < \frac{H_{\mathbf{p}}^{(f)}(s, q)}{s}. \end{aligned} \quad (20)$$

For any fixed \mathbf{p} (12), the positive monotonically decreasing functions $E_{FC}^{(f)}(s, q, R, \mathbf{p})$ and $E_{CR}^{(f)}(s, q, R, \mathbf{p})$ are \cup -convex functions of the parameter $R > 0$ of the following form:

$$E_{FC}^{(f)}(s, q, R, \mathbf{p}) \triangleq \min_{k \in [s]} E_{FC}^{(f)}(s, q, R, \mathbf{p}, k),$$

$$E_{FC}^{(f)}(s, q, R, \mathbf{p}, k) \triangleq \min_{\{\tau\}_k^{(f)}(\mathbf{p})} \left\{ \mathcal{H}^{(f)}(\mathbf{p}, \tau) + [I_k(\mathbf{p}, \tau) - kR]^+ \right\}, \quad (21)$$

and

$$E_{CR}^{(f)}(s, q, R, \mathbf{p}) \triangleq \min_{k \in [s]} E_{CR}^{(f)}(s, q, R, \mathbf{p}, k),$$

$$E_{CR}^{(f)}(s, q, R, \mathbf{p}, k) \triangleq \min_{\{\tau\}^{(f)}} \left\{ \mathcal{H}^{(f)}(\mathbf{p}, \tau) + [I_k(\mathbf{p}, \tau) - kR]^+ \right\}. \quad (22)$$

The minimum in (21) is taken over the subset $\{\tau\}_k^{(f)}(\mathbf{p})$ of distributions $\{\tau\}^{(f)}$ (17) for which the marginal probabilities on x_k are fixed and coincide with $p(x_k)$ (12), $k \in [s]$, i.e.,

$$\{\tau\}_k^{(f)}(\mathbf{p}) \triangleq \{\tau : \tau \in \{\tau\}^{(f)}; \sum_{x_1^{k-1}} \sum_{x_{k+1}^s} \tau(x_1^s, z) = p(x_k), k \in [s]\}. \quad (23)$$

The minimum in (22) is taken over the set of all distributions (17).

Remark 1. Propositions 1-2 and the properties of the random error exponents (19) and (20) were formulated and proved in the papers [2] and [6] for the particular binary case $q = 2$ only. In the general case $q \geq 2$, we omit the proofs because one can check that the given results are based on the same methods developed in [2] and [6]. Here we only note that for the symmetric f -MAC, definitions (21)-(23) leads to the inequality

$$E_{CR}^{(f)}(s, q, R, \mathbf{p}) \leq E_{FC}^{(f)}(s, q, R, \mathbf{p}).$$

Introduce the function

$$E_{FC}^{(f)}(s, q, R) \triangleq \max_{\mathbf{p}} E_{FC}^{(f)}(s, q, R, \mathbf{p}) > 0$$

if $0 < R < C^{(f)}(s, q)$, where $C^{(f)}(s, q)$ is defined in the right-hand side (15). Hence, Propositions 1 and 2 imply that the number $C^{(f)}(s, q)$ can be considered as the Shannon capacity of signature (s, q) -codes for the symmetric f -MAC [5].

The following statement called the random coding lower bound on the rate $R^{(f)}(s, q)$ of signature (s, q) -codes for the symmetric f -MAC can be obtained as a consequence of Proposition 2.

Proposition 3. [6]. *The rate $R^{(f)}(s, q)$ of signature (s, q) -codes for the symmetric f -MAC satisfies the inequality*

$$R^{(f)}(s, q) \geq \underline{R}^{(f)}(s, q), \quad s \geq 2, q \geq 2,$$

where the lower bound $\underline{R}^{(f)}(s, q)$ is

$$\begin{aligned} \underline{R}^{(f)}(s, q) &\triangleq \max_{\mathbf{p}} \min_{k \in [s]} \frac{E_{CR}^{(f)}(s, q, 0, \mathbf{p}, k)}{s + k - 1} = \\ &= \max_{\mathbf{p}} \min_{k \in [s]} \frac{\min_{\{\tau\}_k^{(f)}(\mathbf{p})} \left\{ \mathcal{H}^{(f)}(\mathbf{p}, \tau) + I_k(\mathbf{p}, \tau) \right\}}{s + k - 1} \end{aligned} \quad (24)$$

III. IMPROVEMENTS OF GENERAL BOUNDS

A. Bounds on the Rate $R^{(disj)}(s, 2)$ for the Disjunctive MAC

One can easily see that the capacity of signature $(s, 2)$ -codes for the disjunctive MAC is $C^{(disj)}(s, 2) = 1/s$ and the maximum in the right-hand side of (15) is attained at the distribution \mathbf{p} (12) with $p(0) = 2^{1/s}$ and $p(1) = 1 - 2^{1/s}$. The significant results relative to an improvement of the corresponding entropy bound (15), having the form $R^{(disj)}(s, 2) \leq 1/s$, were obtained in [14] for $s = 2$ and in [13] for $s \geq 11$. In addition, we refer to the best known asymptotic ($s \rightarrow \infty$) lower [6] and upper [13] bounds on the rate $R^{(disj)}(s, 2)$:

$$\frac{2 \ln 2}{s^2} (1 + o(1)) \leq R^{(disj)}(s, 2) \leq \frac{4 \log_2 s}{s^2} (1 + o(1)).$$

B. Bounds on the Rate $R^{(eras)}(s, q)$ for the Erasure MAC

If $q = 2$ and $s \rightarrow \infty$, then it not difficult to establish [16] that the capacity of signature $(s, 2)$ -codes for the erasure MAC is $C^{(eras)}(s, 2) \sim 1/s$ and the maximum in the right-hand side of (15) is asymptotically attained at the symmetric distribution \mathbf{p} (12) with $p(0) \sim \ln 2/s$ or with $p(1) \sim \ln 2/s$. In addition, we refer to the best known asymptotic lower [6] and upper [15] bounds on the rate $R^{(eras)}(s, 2)$:

$$\frac{2 \ln 2}{s^2} (1 + o(1)) \leq R^{(eras)}(s, 2) \leq \frac{4 \log_2 s}{s^2} (1 + o(1)).$$

C. Combinatorial Upper Bound for the Symmetric f -MAC

Theorem 1. *For any symmetric f -MAC, the rate $R^{(f)}(s, q)$ of signature (s, q) -codes satisfies the inequality*

$$R^{(f)}(s, q) \leq \frac{s+1}{2s}, \quad s \geq 2, \quad q \geq 2. \quad (25)$$

Proof of Theorem 1. Fix an arbitrary q -nary $(N \times t)$ -code X_q (1). Without loss of generality we may assume that N is even, i.e., $N = 2k$. Note that all codewords from X_q are distinct. For the given X_q introduce the bipartite graph $G = G(X_q) = (V_1 \cup V_2, E)$ defined as follows. For each vertex in V_1 (as well as in V_2), we put in the correspondence the unique q -nary vector of length k , $|V_1| = |V_2| = q^k$. Two vertices $v_1 \in V_1$ and $v_2 \in V_2$ are connected with an edge iff the code X_q contains a codeword of length $N = 2k$ which is the concatenation of two q -nary vectors of length k , corresponding to v_1 and v_2 . Thus, we obtain the graph $G(X_q)$ having $n = 2q^k = 2q^{N/2}$ vertices and t edges, identified by the elements of $[t]$. In addition, any message $\mathbf{e} \in \mathcal{E}(s, t)$ is interpreted as a non-ordered s -collection of edges.

Let X_q be a q -nary signature (s, q) -code for a symmetric f -MAC. We will check by contradiction that the graph $G(X_q)$ does not contain simple cycles of length $\leq 2s$. Let there exist a simple cycle of the length 2ℓ , $\ell \leq s$. From the cycle we can take the set $E_1 \subset [t]$, $|E_1| = \ell$, of edges, which are not intersected by vertices. Let $E_2 \subset [t]$, $|E_2| = \ell$, $E_1 \cap E_2 = \emptyset$, denote the set of all other edges of the cycle. Consider an arbitrary subset $\mathcal{C} \subset [t] - (E_1 + E_2)$ of the size $|\mathcal{C}| = s - \ell$ and define two messages $\mathbf{e}_i \triangleq E_i + \mathcal{C} \in \mathcal{E}(s, t)$, $i = 1, 2$. It is easy to check that outputs of the symmetric f -MAC for these

messages are the same, i.e., $\mathbf{z}^{(f)}(\mathbf{e}_1, X_q) = \mathbf{z}^{(f)}(\mathbf{e}_2, X_q)$. This contradicts to Definition 1 of signature s -code.

It is known (e.g., see [17]) that if a graph with $n = 2q^{N/2}$ vertices does not contain simple cycles of length $\leq 2s$, then the number t of its edges is

$$t \leq n^{1+1/s} = 2^{1+1/s} q^{N(1+1/s)/2} \leq 4q^{N(1+1/s)/2},$$

i.e., the rate (8) satisfies (25). \square

D. Asymptotic Bounds for the Compositional MAC

For the comp -MAC, the number $H_p^{(\text{comp})}(s, q)$ defined by (13) is called the Shannon entropy of the (s, p) -polynomial distribution. The corresponding maximization problem in the right-hand side (15) was firstly solved in [18], where the author proved that the maximum is attained at the uniform distribution: $p(a) = 1/q$, $a \in \mathcal{A}_q$, i.e.,

$$\begin{aligned} sC^{(\text{comp})}(s, q) &= \max_p H_p^{(\text{comp})}(s, q) = \\ &= \sum_{\{s_0, \dots, s_{q-1}\}} \frac{s! q^{-s}}{s_0! \dots s_{q-1}!} \log_q \frac{s_0! \dots s_{q-1}!}{s! q^{-s}}. \end{aligned} \quad (26)$$

An asymptotic behavior of the right-hand side (26) gives

Lemma 1. *If $s \geq 2$ is fixed and $q \rightarrow \infty$, then the function $sC^{(\text{comp})}(s, q) = s + o(1)$.*

Proof of Lemma 1. From the well-known extremal property of the Shannon entropy (13) it follows

$$sC^{(\text{comp})}(s, q) \leq \log_q |Z| = \log_q \binom{q+s-1}{s} = s + o(1)$$

For $q \geq s$, consider the set \mathcal{Z} , $\mathcal{Z} \subset Z$, of all compositions $\{s_0, \dots, s_{q-1}\}$ with elements $s_a \in \{0, 1\}$. Note that the size $|\mathcal{Z}| = \binom{q}{s}$ and the formula (26) implies that the number

$$sC^{(\text{comp})}(s, q) > \binom{q}{s} \frac{s!}{q^s} \log_q \frac{q^s}{s!}, \quad q \geq s.$$

Hence if $q \rightarrow \infty$, then $sC^{(\text{comp})}(s, q) \geq s + o(1)$. \square

Lemma 1 shows that for the comp -MAC with large parameters s and q , Theorem 1 improves the classical entropy bound (15).

Theorem 2. *If $s \geq 2$ is fixed and $q \rightarrow \infty$, then the rate $R^{(\text{comp})}(s, q)$ of signature (s, q) -codes for the comp -MAC satisfies the asymptotic inequality*

$$\lim_{q \rightarrow \infty} R^{(\text{comp})}(s, q) \geq \frac{s}{2s-1}.$$

Proof of Theorem 2. The proof uses a development of the method which was suggested in [19] and [6] for the binary case $q = 2$. A codeword $\mathbf{x}(j)$, $j \in [t]$, is said to be s -bad for a code X_q in the comp -MAC if there exist m , $m' \in [s]$, and two disjoint messages $\mathbf{e}, \mathbf{e}' \in \mathcal{E}(m, t)$, $\mathbf{e} \cap \mathbf{e}' = \emptyset$, such that

$$j \in \mathbf{e} \quad \text{and} \quad \mathbf{z}^{(\text{comp})}(\mathbf{e}, X_q) = \mathbf{z}^{(\text{comp})}(\mathbf{e}', X_q). \quad (27)$$

Introduce the ensemble of q -nary $N \times t$ matrices X_q , with entries $x_i(j)$ which are chosen independently and equiprobable

from the set \mathcal{A}_q . For the given ensemble, the probability of the event (27) satisfies the inequality

$$\begin{aligned} \Pr\{\mathbf{x}(j) \text{ is } s\text{-bad}\} &\leq \sum_{m=1}^s \binom{t}{2m-1} \times \\ &\times \binom{2m-1}{m} (\Pr\{\text{comp}(u_1^m) = \text{comp}(v_1^m)\})^N, \end{aligned} \quad (28)$$

where the definition (10) along with notations (2) are used and the components of vectors $u_1^m, v_1^m \in \mathcal{A}_q^m$ are independent random variables having the same uniform distribution on the set \mathcal{A}_q . Applying (11), one can write that for any $m \in [s]$,

$$\begin{aligned} \Pr\{\text{comp}(u_1^m) = \text{comp}(v_1^m)\} &= \\ \Pr\left\{\bigcup_{\pi} \left[\bigcap_{i=1}^m (u_i = v_{\pi(i)}) \right]\right\} &\leq \\ \leq m! \cdot \Pr\left\{\bigcap_{i=1}^m (u_i = v_{\pi(i)})\right\} &= \frac{m!}{q^m}. \end{aligned} \quad (29)$$

Inequalities (28)-(29) imply that

$$\begin{aligned} \Pr\{\mathbf{x}(j) \text{ is } s\text{-bad}\} &\leq \\ &\leq s \cdot \max_{m \in [s]} \left[\frac{t^{2m-1}}{m!(m-1)!} \cdot \left(\frac{m!}{q^m} \right)^N \right] \end{aligned} \quad (30)$$

and the standard random coding arguments [6] give

$$R^{(\text{comp})}(s, q) \geq \min_{m \in [s]} \left[\frac{m - \log_q m!}{2m-1} \right].$$

This leads to the statement of Theorem 2. \square

From Theorems 1 and 2 it follows

Corollary 1. *If $s \rightarrow \infty$ and $q \rightarrow \infty$, then the rate $R^{(\text{comp})}(s, q)$ of signature (s, q) -codes for the comp -MAC satisfies the asymptotic equality $R^{(\text{comp})}(s, q) \sim \frac{1}{2}$.*

Remark 2. For the comp -MAC the asymptotic behavior ($q \geq 2$ is fixed, $s \rightarrow \infty$) of upper and lower bounds on the rate $R^{(\text{comp})}(s, q)$ based on Propositions 1-2 was discussed in [6] for $q = 2$ and in [20] for $q \geq 3$.

IV. LIST DECODING CODES FOR JOINABLE MAC

For any s -collection $\mathbf{x}(1), \dots, \mathbf{x}(s)$ of columns $\mathbf{x}(j) \in \mathcal{A}_q^N$, $j \in [s]$, introduce its *joining*

$$\langle \mathbf{x}(j), j \in [s] \rangle \triangleq \left(\bigcup_{j=1}^s x_1(j), \dots, \bigcup_{j=1}^s x_N(j) \right),$$

which is a column of N subsets of \mathcal{A}_q . We say that a column $\mathcal{Q} = (\mathcal{Q}_1, \dots, \mathcal{Q}_N)$, $\mathcal{Q}_i \subseteq \mathcal{A}_q$, $i \in [N]$, *covers* a column $\mathbf{x} = (x_1, \dots, x_N) \in \mathcal{A}_q^N$ if $x_i \in \mathcal{Q}_i$ for any $i \in [N]$.

Definition 3. [15]. A q -ary code X_q (1) is said to be a *list-decoding* (s_L, q) -code of size t and length N for *join*-MAC if for any s -collection of codewords $(\mathbf{x}(j_1), \dots, \mathbf{x}(j_s))$ its joining $\langle \mathbf{x}(j_k), k \in [s] \rangle$ covers not more than $L - 1$ other codewords of code X_q .

In the case $L = 1$ the list-decoding (s_1, q) -code (or s -frameproof code [21]) is a signature (s, q) -code for join-MAC. Moreover, list-decoding (s_1, q) -code provides a simpler factor decoding algorithm, that picks the unknown message $\mathbf{e} \in \mathcal{E}(s, t)$ by searching all codewords of X_q covered by the output signal $\mathbf{z}^{(join)}(\mathbf{e}, X_q) = \langle \mathbf{x}(\mathbf{e}) \rangle$. In the general case $L \geq 1$, the algorithm gives a subset of $[t]$ that contains s transmitted elements and not more than $L - 1$ extra elements.

Let $t(s_L, q, N)$ be the maximal possible size of list-decoding (s_L, q) -codes of length N . For fixed $s \geq 2$, $L \geq 1$ and $q \geq 2$, define a rate of list-decoding (s_L, q) -codes:

$$R(s_L, q) \triangleq \lim_{N \rightarrow \infty} \frac{\log_q t(s_L, q, N)}{N}.$$

In [15] the author establishes a random coding bound on the rate of list-decoding (s_L, q) -codes, which improves the best previously known bounds presented in [16], [22], [23].

Theorem 3. [15]. 1. For any fixed $q \geq 2$, $s \geq 2$ and $L \geq 1$ the following lower bound holds:

$$R(s_L, q) \geq \underline{R}(s_L, q) \triangleq \max_{q' \geq q} \frac{-\log_q P(q', s, L)}{(s + L - 1)k(q, q')}, \quad (31)$$

where

$$P(q, s, L) \triangleq \sum_{m=1}^{\min\{q, s\}} \binom{q}{m} \left(\frac{m}{q}\right)^L \times \sum_{k=0}^m (-1)^k \binom{m}{k} \left(\frac{m-k}{q}\right)^s, \quad (32)$$

$$k(q, q') \triangleq \begin{cases} 1, & \text{for } q = q', \\ \lceil \frac{q'}{q-1} \rceil, & \text{otherwise.} \end{cases} \quad (33)$$

2. For any fixed $q \geq 2$, $L \geq 1$ and $s \rightarrow \infty$

$$\underline{R}(s_L, q) = \frac{L(q-1) \log_q e}{s^2 (\log_2 e)^2} (1 + o(1)), \quad s \rightarrow \infty. \quad (34)$$

3. For any fixed $s \geq 2$ and $L \geq 1$ there exists a limit

$$\lim_{q \rightarrow \infty} \underline{R}(s_L, q) = \frac{L}{s + L - 1}. \quad (35)$$

In [15] it was also conjectured that the lower bound (35) is precise. We prove the conjecture in

Theorem 4. For any $s \geq 2$, $L \geq 1$ and $q \geq 2$ the rate $R(s_L, q)$ of list-decoding (s_L, q) -codes for join-MAC satisfies the asymptotic inequality

$$R(s_L, q) \leq \frac{L}{s + L - 1}. \quad (36)$$

Proof of Theorem 4. Consider an arbitrary code X_q of length N and size t . For a convenience of the proof, we will use indexes j (i) of codewords (rows) which can exceed t (N), assuming that the indexes (coordinates) are cyclically ordered, i.e., for instance, if a row index $n > N$, then for any $j \in [t]$, the symbol $x_n(j) \triangleq x_{n'}(j)$, where $n' \triangleq n \bmod N$. For a codeword $\mathbf{x}(j) \in \mathcal{A}_q^N$, $j \in [t]$, we say that the symbol

$$\mathbf{x}_i^{i+L-1}(j) \triangleq (x_i(j), \dots, x_{i+L-1}(j)) \in \mathcal{A}_q^L, \quad i \in [N],$$

denotes a projection of the codeword $\mathbf{x}(j)$ on the coordinates $i, i+1, \dots, i+L-1$. A codeword $\mathbf{x}(j)$, $j \in [t]$, is said to be an L -rare in X_q if there exists a row index $i \in [N]$ such that the number of codeword indexes $j', j' \in [t]$, $j' \neq j$, such that the projection $\mathbf{x}_i^{i+L-1}(j') = \mathbf{x}_i^{i+L-1}(j)$, does not exceed $L-1$. Let $r = r_L(X_q)$ be the number of codewords which are L -rare in X_q . For each L -rare $\mathbf{x}(j)$, we can choose a number $i \in [N]$, a q -nary L -sequence $(a_1, \dots, a_L) \in \mathcal{A}_q^L$ and an ordinal number of the $\mathbf{x}(j)$ among all $\leq L$ codewords $\mathbf{x}(j')$, $j' \in [t]$, for which $\mathbf{x}_i^{i+L-1}(j') = \mathbf{x}_i^{i+L-1}(j) = (a_1, \dots, a_L)$. Therefore, the following claim holds.

Lemma 2. For any code X_q of length N , the number $r_L(X_q)$ of its L -rare codewords satisfies the inequality

$$r = r_L(X_q) \leq N L q^L. \quad (37)$$

Lemma 3. If a q -nary code X_q of length N has a size

$$t > N L q^L \sum_{n=0}^{L-1} n!, \quad (38)$$

then there exists a subset $\mathcal{L}_s = \{j_1, \dots, j_L\} \subset [t]$ of the size $|\mathcal{L}_s| = L$, such that the L -sequence $\{\mathbf{x}(j), j \in \mathcal{L}_s\}$ does not contain codewords which are L -rare in X_q . In addition, for any $k \in [L-1]$ the projections of $\mathbf{x}(j_k)$ and $\mathbf{x}(j_{k+1})$ on the coordinates $1+k(s-1), 2+k(s-1), \dots, L+k(s-1)$ are the same, i.e.,

$$\mathbf{x}_{1+k(s-1)}^{L+k(s-1)}(j_k) = \mathbf{x}_{1+k(s-1)}^{L+k(s-1)}(j_{k+1}), \quad k \in [L-1]. \quad (39)$$

Proof of Lemma 3. For any $j_1 \in [t]$, we try to construct a sequence $\mathcal{L}(j_1) = \{\mathbf{x}(j_1), \mathbf{x}(j_2), \dots, \mathbf{x}(j_L)\}$ of L codewords by the following rules. The first element of the sequence $\mathcal{L}(j_1)$ is equal to $\mathbf{x}(j_1)$. Let a sequence $\{\mathbf{x}(j_1), \mathbf{x}(j_2), \dots, \mathbf{x}(j_k)\}$ of a length k , $1 \leq k \leq L$, be constructed. If the last codeword $\mathbf{x}(j_k)$ is L -rare in X_q , then the process ends with a failure. If $k = L$ and $\mathbf{x}(j_L)$ is not L -rare in X_q , then the process successfully ends. Otherwise, for $k \leq L-1$, we consider L indexes from $1+k(s-1)$ to $L+k(s-1)$. Since the codeword $\mathbf{x}(j_k)$ is not L -rare in X_q we can find at least L another codewords with the same projection on the coordinates from $1+k(s-1)$ to $L+k(s-1)$. Among them there are $\leq k-1 \leq L-2$ codewords that could be already included in the sequence at the previous $k-1$ steps. Therefore, there exists a codeword, which has not been used. Among all such unused codewords, we uniquely choose the codeword $\mathbf{x}(j_{k+1})$ with the cyclically smallest index j_{k+1} , $j_{k+1} > j_k$, as a next element of $\mathcal{L}(j_1)$.

Let us prove, that there exists a codeword $\mathbf{x}(j_1)$, such that the described process will successfully end, i.e., as a result, we obtain a sequence $\mathcal{L}(j_1)$ without L -rare codewords. The only reason of a failure is an emergence of an L -rare codeword. Fix an arbitrary L -rare codeword $\mathbf{x}(j)$. Suppose that for some j_1 and sequence $\mathcal{L}(j_1)$ we constructed $\mathbf{x}(j_n) = \mathbf{x}(j)$, $n \leq L$. By construction of the sequence $\mathcal{L}(j_1)$ we know that the codeword $\mathbf{x}(j_n)$ has the cyclically smallest index $j_n > j_{n-1}$ among all

codewords, except $\mathbf{x}(j_1), \dots, \mathbf{x}(j_{n-2})$, and coincides with the codeword $\mathbf{x}(j_{n-1})$ on the L coordinates:

$$1 + (n-1)(s-1), 2 + (n-1)(s-1), \dots, (L-1) + (n-1)(s-1), L + (n-1)(s-1). \quad (40)$$

Hence, the codeword $\mathbf{x}(j_{n-1})$ is the first codeword before $\mathbf{x}(j_n)$, except $\mathbf{x}(j_1), \dots, \mathbf{x}(j_{n-2})$, which has the same symbols as $\mathbf{x}(j_n)$ on the L coordinates (40). The number of codewords among $\mathbf{x}(j_1), \dots, \mathbf{x}(j_{n-2})$, which have the same symbols as $\mathbf{x}(j_n)$ and $\mathbf{x}(j_{n-1})$ on the L coordinates (40) is from 0 to $n-2$. Therefore, for fixed codeword $\mathbf{x}(j_n)$ there exist $\leq n-1$ of possible variants for $\mathbf{x}(j_{n-1})$. Thus, any L -rare codeword $\mathbf{x}(j)$, uniquely chosen as the codeword $\mathbf{x}(j_n)$ in the sequence $\mathcal{L}_s(j_1)$, spoils $\leq (n-1)!$ of starting codewords $\mathbf{x}(j_1)$. In virtue of condition (38) and upper bound (37) from Lemma 2, the code size $t > r_L(X_q) \cdot \sum_{n=0}^{L-1} n!$. Therefore, there exists a starting codeword $\mathbf{x}(j_1)$, such that the sequence $\mathcal{L}(j_1)$ will be successfully constructed and can be written in the form $\{\mathbf{x}(j), j \in \mathcal{L}_s\}$, $|\mathcal{L}_s| = L$. \square

Lemma 4. For any list-decoding (s_L, q) -code X_q of the length $N = s + L - 1$, the size t of the code X_q is upper bounded as follows:

$$t \leq (s + L - 1) L q^L \sum_{n=0}^{L-1} n!. \quad (41)$$

Proof of Lemma 4. Consider an arbitrary list-decoding (s_L, q) -code X_q of the length $N = s + L - 1$. We prove the claim of Lemma 4 by contradiction. Assume that $t > (s + L - 1) L q^L \sum_{n=0}^{L-1} n!$. In virtue of Lemma 3, it is sufficient to construct the subset $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, such that the joining $\langle \mathbf{x}(j), j \in \mathcal{S} \rangle$ covers every codeword of the sequence $\mathcal{L}(j_1) = \{\mathbf{x}(j), j \in \mathcal{L}_s\}$, $\mathcal{L}_s = \{j_1, \dots, j_L\}$, constructed in the proof of Lemma 3. Define a sequence \mathcal{P} of pairs, where each pair represents the index j_k of codeword $\mathbf{x}(j_k)$ and the coordinate i in this codeword, such that the symbol $x_{i(j_k)}$ should be covered by the joining $\langle \mathbf{x}(j), j \in \mathcal{S} \rangle$:

$$\begin{aligned} \mathcal{P} = \{ & (j_1, 1), (j_1, 2), \dots, (j_1, N), (j_2, L + 1 + (s-1)), \dots \\ & (j_2, L + 1 + 2(s-1)), \dots, (j_k, L + 1 + (k-1)(s-1)) \dots \\ & (j_k, L + k(s-1)), \dots, (j_L, sL) \}. \end{aligned}$$

Divide this sequence of pairs into s groups g_k , $k \in [s]$, according to the order of their appearance in the sequence \mathcal{P} , i.e.

$$g_k \triangleq \{(j_{k_1}, i_{k_1}), \dots, (j_{k_L}, i_{k_L})\}, \quad \{j_{k_1}, \dots, j_{k_L}\} \subset \mathcal{L}_s.$$

Firstly, note that the projection $\mathbf{x}(j_{k_L})$ on the coordinates $i_{k_1}, i_{k_2}, \dots, i_{k_L}$ is

$$\begin{aligned} (x_{i_{k_1}}(j_{k_1}), x_{i_{k_2}}(j_{k_2}), \dots, x_{i_{k_L}}(j_{k_L})) = \\ = (x_{i_{k_1}}(j_{k_L}), x_{i_{k_2}}(j_{k_L}), \dots, x_{i_{k_L}}(j_{k_L})). \end{aligned}$$

Secondly, from the construction of the set \mathcal{L}_s described in the proof of Lemma 3 it follows that codeword $\mathbf{x}(j_{k_L})$ is not L -rare. Therefore, we can find an index l_k , $l_k \notin \mathcal{L}_s$, and

the corresponding codeword $\mathbf{x}(l_k)$ such that the projections of $\mathbf{x}(l_k)$ and $\mathbf{x}(j_{k_L})$ on the coordinates $i_{k_1}, i_{k_2}, \dots, i_{k_L}$ are the same, i.e.,

$$\begin{aligned} (x_{i_{k_1}}(j_{k_L}), x_{i_{k_2}}(j_{k_L}), \dots, x_{i_{k_L}}(j_{k_L})) = \\ = (x_{i_{k_1}}(l_k), x_{i_{k_2}}(l_k), \dots, x_{i_{k_L}}(l_k)) \quad k \in [s]. \quad (42) \end{aligned}$$

In addition, the property (42) implies that the joining $\langle \mathbf{x}(l_k), k \in [s] \rangle$ covers the sequence $\mathcal{L}(j_1) = \{\mathbf{x}(j), j \in \mathcal{L}_s\}$. The obtained contradiction proves Lemma 4. \square

The proof of Lemma 4 is intuitively illustrated by the following two examples.

Example 1. Let $L = s = 3$ and $N = L + s - 1 = 5$. Then three q -nary codewords $\mathbf{x}(j_k), \mathbf{x}(l_k) \in \mathcal{A}_q^5$, $k \in [3]$, satisfying the equalities (39) can be written in the form:

$$\begin{aligned} \mathbf{x}(j_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)), \\ \mathbf{x}(j_2) &= (y_2, z_2, x_3(j_1), x_4(j_1), x_5(j_1)), \\ \mathbf{x}(j_3) &= (y_2, z_2, y_3, z_3, x_5(j_1)). \end{aligned}$$

These codewords are covered by the joining of three q -nary codewords $\mathbf{x}(l_k), \mathbf{x}(l_k) \in \mathcal{A}_q^5$, $k \in [3]$, which are based on the property (42) and can be written in the form:

$$\begin{aligned} \mathbf{x}(l_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), a_1, a_2), \\ \mathbf{x}(l_2) &= (y_2, b_1, b_2, x_4(j_1), x_5(j_1)), \\ \mathbf{x}(l_3) &= (c_1, z_2, y_3, z_3, c_2). \end{aligned}$$

Example 2. Let $L = 4$, $s = 2$ and $N = L + s - 1 = 5$. Then four q -nary codewords $\mathbf{x}(j_k), \mathbf{x}(l_k) \in \mathcal{A}_q^5$, $k \in [4]$, satisfying the equalities (39) can be written in the form:

$$\begin{aligned} \mathbf{x}(j_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)), \\ \mathbf{x}(j_2) &= (y_2, x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)), \\ \mathbf{x}(j_3) &= (y_2, y_3, x_3(j_1), x_4(j_1), x_5(j_1)), \\ \mathbf{x}(j_4) &= (y_2, y_3, y_4, x_4(j_1), x_5(j_1)). \end{aligned}$$

These codewords are covered by the joining of two q -nary codewords $\mathbf{x}(l_k), \mathbf{x}(l_k) \in \mathcal{A}_q^5$, $k \in [2]$, which are based on the property (42) and can be written in the form:

$$\begin{aligned} \mathbf{x}(l_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), a_1), \\ \mathbf{x}(l_2) &= (y_2, y_3, y_4, a_2, x_5(j_1)). \end{aligned}$$

To complete the proof of Theorem 4, consider an arbitrary list-decoding (s_L, q) -code X_q of length N , $N > s + L - 1$, and size t . Divide each codeword of the code X_q into $s + L - 1$ parts of sizes

$$n_i, \quad \left\lfloor \frac{N}{s + L - 1} \right\rfloor \leq n_i \leq \left\lceil \frac{N}{s + L - 1} \right\rceil, \quad i \in [s + L - 1].$$

The number of different parts is upper bounded by the sum $q^{\lfloor \frac{N}{s+L-1} \rfloor} + q^{\lceil \frac{N}{s+L-1} \rceil}$. Replace each part of each codeword with a unique symbol from the Q -nary alphabet of the size $Q \triangleq 2q^{\lceil \frac{N}{s+L-1} \rceil}$. It is easy to see that the obtained code X_Q is a Q -nary list-decoding (s_L, Q) -code of the length

$N = s + L - 1$ and the size t . Thus, the inequality (41) of Lemma 4 implies that the size

$$t \leq (s + L - 1)L \sum_{n=0}^{L-1} n! 2^L q^{L \lceil \frac{N}{s+L-1} \rceil}.$$

The obtained upper bound immediately leads to (36). \square

ACKNOWLEDGMENT

The research is supported in part by the Russian Foundation for Basic Research under Grant No. 16-01-00440 a.

REFERENCES

- [1] Csiszar I., Korner J.: Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge University Press (2011).
- [2] D'yachkov A.G., Bounds on error probability for the symmetric model of designing screening experiments. *Probl. Inf. Trans.*, 1981, **17**:4, 245-263.
- [3] Gyofri, L., Gyofri, S., Laczay, B., Ruzinko, M. Lectures on multiple access channels. Web: http://www.szit.bme.hu/gyofri/AFOSR_05.
- [4] D'yachkov A.G., Rykov V.V., On a Coding Model for a Multiple-Access Adder Channel. *Probl. Inf. Trans.*, 1981, **17**:2, 94-104
- [5] M.B. Maljutov and P. Mateev, Design of screening experiments with non-symmetric response function. *Mathematical Notes*, 1980, **27**:1, 57-68.
- [6] D'yachkov A.G., Lectures on Designing Screening Experiments, Lecture Note Series 10, Combinatorial and Computational Mathematics Center, Pohang University of Science and Technology, Korea Republic, Feb. 2003 (survey, 112 pages).
- [7] Chang S.C. and Wolf J.K., "On the T-user M-frequency noiseless multiple-access channel with and without intensity information", *IEEE Trans. Inf. Theory*, 1981, **27**:1, 41-48.
- [8] Bassalygo, L.A. and Pinsker, M.S., Evaluation of the Asymptotics of the Summarized Capacity of an M-Frequency T -User Noiseless Multiple-Access Channel, *Probl. Inf. Trans.*, 2000, **36**:2, 91-97.
- [9] Frolov, A. A., and Zyablov, V. V. (2014). On the capacity of a multiple-access vector adder channel. *Probl. Inf. Trans.*, 2014, **50**:2, 133-143.
- [10] Wilhelmsson, L. and Zigangirov, K.Sh., On the Asymptotic Capacity of a Multiple-Access Channel, *Probl. Inf. Trans.*, 1997, **33**:1, 9-16.
- [11] Han Vinck, A.J. and Keuning, J., On the Capacity of the Asynchronous T -User M-Frequency Noiseless Multiple-Access Channel without Intensity Information, *IEEE Trans. Inform. Theory*, 1996, **42**:6, 2235-2238.
- [12] Du D.Z., Hwang F.K., Combinatorial Group Testing and Its Applications, 2nd ed. // Series on Applied Mathematics, **12**, 2000.
- [13] D'yachkov A.G., Vorobyev I.V., Polyanskii N.A., Shchukin V.Yu., Bounds on the Rate of Disjunctive Codes, *Probl. Inf. Trans.*, 2014, **50**:1, 31-63.
- [14] Copperer-Smith D., Shearer J. New Bounds for Union-free Families of Sets // *The Electronic Journal of Combinatorics*, 1998, **5**:1, R39.
- [15] Shchukin V.U., List decoding in a hyper multiple access channel, *Probl. Inf. Trans.*, 2016, **52**:4, 329-343.
- [16] Rashad A.M., On Symmetrical Superimposed Codes, *J. Inf. Process. Cybern EIK*, 1989, **29**:7, 337-341.
- [17] Bondy, John A., and Mikls Simonovits. "Cycles of even length in graphs." *Journal of Combinatorial Theory, Series B*, 1974, **16**:2, 97-105.
- [18] Mateev P.S., On the Entropy of the Polynomial Distribution, *Theory Probab. Appl.*, 1978, **23**:1, 188-190.
- [19] Poltyrev G.Sh., On an improvement of upper bounds to error probability for codes with complicated structure, *Probl. Inf. Trans.*, 1987, **23**:4, 251-262.
- [20] Egorova, E., Potapova, V. Signature codes for a special class of multiple access channel. In *Problems of Redundancy in Information and Control Systems*, 2016 XV International Symposium, pp. 38-42.
- [21] Boneh D. and Shaw J., "Collusion-secure fingerprinting for digital data", *IEEE Trans. Inf. Theory*, 1998, **44**:5, 1897-1905.
- [22] Shangguan C., Wang X., Ge G., Miao Y., New Bounds For Frameproof Codes, Preprint, 2014. <http://arxiv.org/pdf/1411.5782> v1.
- [23] Stinson D.R., Wei R., Chen K., On generalized separating hash families, *J. Combin. Theory, Ser. A*, 2008, **115**:1, 105-120.